# THE CYBER SHIELD

*Cyber News for Counterintelligence / Information Technology / Security Professionals*

*25 June 2014*

**Purpose**
Educate recipients of cyber events to aid in protecting electronically stored DoD, corporate proprietary, and/or Personally Identifiable Information from theft, compromise, espionage

**Source**
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

**Publisher**
* SA Jeanette Greene
Albuquerque FBI

**Editor**
* CI SA Scott Daughtry
DTRA Counterintelligence

**Subscription**
To receive this newsletter please send an email to scott.daughtry@dtra.mil

**Disclaimer**
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

**NMCIWG Members**
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, and Sandia National Labs

**Distribution**
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings. Credit is given to the NMCIWG for the compilation of this open source data

*June 24, IDG News Service* – (International) **New Havex malware variants target industrial control system and SCADA users.** Researchers with F-Secure reported June 23 that attackers have been distributing new versions of the Havex remote access trojan (RAT) by compromising industrial control system (ICS) manufacturers' Web sites and adding the RAT to legitimate software downloads. The researchers did not name the manufacturers but stated that they are based in Belgium, Germany, and Switzerland. Source: http://www.networkworld.com/article/2367241/new-havex-malware-variants-target-industrial-control-system-and-scada-users.html

*June 24, Threatpost* – (International) **Researchers go inside HackingTeam mobile malware, command infrastructure.** Researchers from Kaspersky Lab and the University of Toronto reported findings of research into the Remote Control System (RCS) or Galileo malware created and sold by the HackingTeam company to various governments and law enforcement agencies, including the malware's command and control (C&C) infrastructure and mobile malware components for Android and iOS devices. The researchers also found that the majority of the C&C servers were hosted in the U.S., U.K., Canada, Ecuador, and Kazakhstan. Source: http://threatpost.com/researchers-go-inside-hackingteam-mobile-malware-command-infrastructure

*June 24, The Register* – (International) **Comcast Xfinity evil twin steals subscriptions.** A researcher at LogRhythm Labs demonstrated how an attacker could compromise Comcast Xfinity accounts by creating a malicious hotspot that mimics Comcast customer-run hotspots, and that Comcast customer devices would automatically connect to. The malicious hotspot then presents a legitimate-looking login page that collects a customer's login and password. Source: http://www.theregister.co.uk/2014/06/24/comcast_xfinity_evil_twin_steals_subcriptions/

**WiFi SSID and Passcode for World Cup Security Center Exposed in Newspaper**
SoftPedia, 25 Jun 2014: The picture with the log-in information was published in Correio Braziliense, a local newspaper, showing Luiz Cravo Dorea, head of international cooperation. Behind him, on a monitor wall, was the secret information that can be read with a squint of the eye. The SSID is World Cup and the identified log-in password is "b5a2112014." It looks like a secure one, but a brief look tells more tech-savvy users that it is actually leet speak for "brazil2014." The security center is used for watching video feeds from the cameras strategically positioned around the competition venues. It is run by an Israeli company part of the RISCO group for coordinating hundreds of security cameras. The password for connecting to the WiFi network has been changed, and probably the SSID, too, but the fact that the sensitive information was available in plain view and captured in a photo does question the security measures taken at the event. The image was posted on Twitter and has been shared almost 2,500 times. Some users speculate that its being available in the open could be intentional and that the organizers intended it as a honeypot. Wanna know the pwd for the Brasil world cup security center WiFi nw? It's on the whiteboard ;-) #fail pic.twitter.com/XD6ujqk5nq — Augusto Barros (@apbarros) June 23, 2014 However, it appears that the newspaper publishing the image has already changed it. To read more click **HERE**

### Microsoft Releases Security Improvements for Windows Update

SoftPedia, 25 Jun 2014: Microsoft has recently announced a new security patch for Windows Update specifically supposed to increase protection of the customers receiving the updates and to ensure a more secure communication between the client and the server. Basically, all new Windows operating systems are getting this new pack of improvements, including Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1, Windows 8, Windows RT, and Windows Server 2012. The rollout officially started on June 23 and will continue in the coming weeks to make sure that all computers running any of the aforementioned operating system versions are getting it. Microsoft says that this is an automatic update, so unless you have turned the automatic updates off on your computer, the patch might already be there waiting for a reboot. "Similar to past updates, this update will be automatically installed if Automatic Updates is turned ON, either set to automatically install updates or notify to download/install updates," the company explains in a post. No settings will be changed on your computer and the update will be automatically deployed, as long as automatic updates are turned on, Microsoft further notes. "As with past updates, this update will not change your current Windows Update or Automatic Updates settings. Anytime Windows Update (or Automatic Updates) is turned ON, either set to automatically install updates or notify to download/install updates, Windows Update will take care of updating itself," it said. According to information posted in KB2887535, the new patch for Windows Update includes hardening of infrastructure used by WU/MU client and a more secure communication channel between WU/MU Client and Service, which could actually be used by future updates prepared for Windows workstations. As you might have heard, Microsoft is working on a second update for Windows 8.1, so these improvements might actually be used by the future release in order to successfully install on all computers. In the past, both Windows 8.1 and 8.1 Update were hit by installation issues that prevented some computers from receiving it, even though the company promised a seamless experience for everyone. Most of these issues have been fixed afterward, but there's no doubt that both users and the company expect future OS updates to install more smoothly on their machines. Windows 8.1 Update 2 is expected to be released in August or September, so make sure that you install these new improvements by that time. To read more click HERE

### 97,000 Patient Files Accessed by NRAD Employee

SoftPedia, 25 Jun 2014: A NRAD radiologist accessed without authorization the files of 97,000 patients, containing personally identifying information, including social security numbers. The employee, who was reported to the authorities, managed to breach the security systems protecting the company's billing and data information and access records and details about the patients' health. According to the investigation initiated as a result of the incident, it appears that the files contained dates of birth, addresses, social security numbers, health insurance information, diagnoses and procedure codes. In a letter to the affected parties, the company notes that it has no knowledge of financial information having been accessed or that the details in the files have been disclosed or used by a third party. The number of patient files the radiologist had access to represents 12% of the more than 800,000 patients treated in the last 20 years. When the breach was discovered, on or about April 24, security measures were immediately upgraded to new standards. NRAD offered the affected individuals free credit inquiry service from three major credit bureaus that can be contacted if signs of credit card fraud are noticed. Although this incident may be considered of low risk, social security numbers are a valuable asset for cybercriminals, as they can use them to commit identity theft and fraud. To read more click HERE